~~TOP SECRET~~

~~TOP SECRET~~

APR 20 1951

MEMORANDUM FOR BRIGADIER JOHN H. TILTMAN

Subject: Staff Study on the Improvement of French Communications

1. There is forwarded for your information a staff study prepared by AFSA for use in the forthcoming US-UK conference on improvement of French communications.

2. In a message received through USLO the Director, GCHQ, requested that U.S. views concerning items on the agenda be forwarded to arrive not later than 22 April. I believe the staff study will provide the information he desires. In view of the short time available, it would be appreciated if you would forward the staff study to the Director, GCHQ, by SECRATYPE or ROCKEX.

S. P. COLLINS
Colonel, Signal Corps
Deputy Director, AFSA

1 Incl
Staff Study on the Improvement of French Communications, dated 20 April 1951 (3 copies)

cc: AFSA-00B
AFSA-00A
AFSA-123
AFSA-00T

Col S.P.Collins/AFSA-00A
20 Apr 51/mcg/60535

~~TOP SECRET~~

DRAFT

STAFF STUDY ON THE IMPROVEMENT OF FRENCH COMMUNICATIONS

THE PROBLEM

1. In preparation for a US-UK conference on the subject, to examine present French cryptographic systems and procedures, and to formulate a U.S. plan for improvement of the security thereof.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure "B."

CONCLUSIONS

3. It is concluded that:

[redacted]

b. The present French cryptographic organizations do not possess the necessary cryptanalytic appreciation to insure provision of systems affording adequate cryptographic security, or, if they do possess the requisite knowledge, the information is not being applied or properly employed.

c. This situation can be corrected only by a complete overhaul of the French cryptographic systems and practices. The present insecure French cryptographic systems and practices should be replaced by secure systems and practices, and a specific plan for such replacement should be established.

d. Positive measures to effect such a plan should be introduced even to the extent of providing, at least in part, the cryptographic devices and associated techniques essential to security.

e. This will materially reduce the amount of intelligence now available to Russia from COMINT sources probably exploitable by them; it

[redacted]

f. Negotiations with the French should be conducted in such a manner that there is [redacted]

g. As a preliminary to entering upon any negotiations with the French there should be reasonable assurance that the effects of improving their communication security will not be nullified or diminished by physical and personnel insecurity in the French Government. It is obvious that without such assurance [redacted] without any compensating gains in security.

h. The bases for a successful approach to the French Government cannot yet be indicated and should be established in the discussions at the U.S.-U.K. Conference soon to convene in Washington.

ENCLOSURE "A"

PLAN FOR IMPROVING THE CRYPTOGRAPHIC SECURITY OF FRENCH COMMUNICATIONS

A. DIPLOMATIC:

1. The proposal presented herein for ensuring the security of French Diplomatic communications considers that the various French diplomatic posts should be subdivided into three categories:

a. Category I: A small group of locations which handle the most critical information, such as Paris, London, and Washington.

b. Category II: All capitals not included in a. plus a selected group of important cities whose communications frequently include information of considerable intelligence value.

c. Category III: All other diplomatic posts.

2. The systems recommended, respectively, for the three categories listed above are:

a. For Category I: The Combined Cipher Machine with Simplex settings. The word Simplex is used to mean a procedure whereby each message has its own rotor arrangement and alignment provided by means of a special key list. The lists are prepared for point-to-point use so that each station can read only those messages specifically addressed to it. For the exceptional cases of multiple-address messages, a multiple holder key list is provided. A one-time pad system should be provided as an emergency stand-by in this category.

b. For Category II: The M-209 with special settings used to encipher messages set up in a literal code. The code book used should be a new book specially designed for this sole purpose. Each holder in this category should be provided with three distinct systems; one for use solely with Paris, one for use laterally on a limited regional basis, and one for use laterally on a world wide basis.

c. For Category III: Present French systems would continue to be used.

3. The stations in each category will be included as holders in the categories below them.

4. The localization introduced by Simplex procedures in Category I and by special or area settings in Category II has a double advantage. First, it increases the cryptosecurity generally; and secondly, if there should be an instance of penetration by the Russians which grants access to cryptographic information, the dangers resulting from such penetration are confined to the single cryptonet involved. This results in minimizing the consequent loss of information.

5. The merit of these proposals is the provision of a fairly high degree of security for French Diplomatic and highest-level NATO communications, together with a minimum disclosure to the French of systems and ideas with which they are not already familiar. For the transmission of international Diplomatic or highest-level Military traffic dealing with Western Union and NATO affairs, they have been provided with TYPEX machines and they are presently using a Simplex procedure with these machines in the highest echelons of NATO; the Combined Cipher Machine is also being offered to them, as well as to other NATO signatories, for NATO communications; French Army, Navy, and Air Force personnel are familiar with and have some copies of the M-209, so that they have experience in the preparation of M-209 settings and can instruct French diplomatic officials in the use of the M-209. Adequate training in the new systems will therefore be greatly simplified as a result of the already-existing familiarity with them.

6. The establishment of appropriate communications security procedures will be facilitated by the issue of JANAP 122(B) (the U.S. Joint Manual on Communications Security), which is presently under consideration for use in connection with NATO cryptographic systems.

B. ARMED SERVICES:

7. Authorities concerned with NATO communications have already established two categories of such communications:

a. Category I (High-level): This category embraces the top-level military representatives of each nation of NATO. For this level, the British TYPEX machine, with Simplex settings is being used. Consideration is being given to adapting that machine to a NATO CCM system.

b. Category II (Intermediate-level): This category embraces military headquarters down to and including Division headquarters or equivalent. For the level the U.S. and the U.K. have proposed the CCM, and the proposal is now under consideration by the other NATO governments.

8. There remains for consideration purely French national military (Army, Navy, Air Force) communications of a level below that of 7b above. For this level, which would constitute Category III, the use of M-209, to encipher plain language (not code groups as in the case of Category II of the plan for the Diplomatic communications provided for in paragraph 2b above) would probably be acceptable to the U.S.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

[redacted]

2. In regard to the current French Diplomatic communications, observed French practices in cryptographic system design and distribution provide direct evidence that the present cryptographic organization in the French Diplomatic Service does not possess the necessary cryptanalytic appreciation to insure provision of systems affording adequate cryptographic security, or, if it does possess the requisite knowledge, the information is not being applied or properly employed, either in the Foreign Ministry or in Diplomatic posts. Except as regards certain systems, which may be one-time pad, none of the French Diplomatic cryptographic systems possesses sufficient inherent security to permit its improvement to a point where it might be considered acceptable. It would therefore be necessary to discard the current systems

and replace them with other systems based on sounder cryptographic principles. It would also be necessary to provide technically sound associated procedures and training in the proper use of the systems and procedures.

4. Although a tradition of sound communication security doctrine did exist in France, the current cryptographic practices observed in French Diplomatic traffic indicate that the French have fallen far behind the U.S. and the U.K. in matters pertaining to communication security. The situation is less serious in the Army, but there too there is much room for improvement. Therefore, technical assistance from outside the French cryptographic services is deemed essential for the success of any communication security program.

5. From an over-all consideration it may be stated that if the security of French Diplomatic and Military communications is to be improved it would be necessary to:

a. Replace the current French cryptographic systems with secure systems for use in all important diplomatic posts and in the headquarters of all high-echelon military units.

b. Establish technically sound communications security procedures.

c. Insure adequate training in the use of the new systems and procedures.

d. Insure careful technical supervision over French communications to maintain communication security.

6. In view of the foregoing, it is apparent that a complete overhaul of the French Diplomatic and Military cryptographic systems and practices would be necessary. This would involve not only informing the French that their present systems are insecure but also establishing a basis on which the French would be provided with appropriate technical assistance to enable them to reorganize their cryptographic systems and practices to insure secure communications.

7. It is obvious that in assisting the French in improving the security of their cryptographic communications [redacted] However, (a) the necessity for removing those handicaps to proper diplomatic discussions and negotiations between the U.S. and the French Governments which arise from present insecurity of French Diplomatic communications, and (b) the importance of denying to Russia this source of COMINT, make it in the interest of the U.S. and the U.K. [redacted] and also to provide, at least in part, the cryptographic devices and associated techniques essential to security.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

[redacted]

9. The possibility of Russian penetration of some or all of the French services, both diplomatic and military, cannot be ignored. Penetration may ~~be either complete or partial, and may~~ extend into ~~either~~ (a) the sources of information or ~~into~~ (b) or (c), both. the cryptographic services. ~~Complete~~ penetration of any of these ~~either~~ three types would ~~make totally ineffective~~ discount the value of any plan for improving cryptographic security. [redacted] the sacrifice would not necessarily be accompanied by a denial of ~~without denying~~ information to the Russians. Therefore, before any steps are taken, there should be reasonable assurance of adequate physical and personnel security in the French Foreign Office, the French Armed Services, and the offices which control the cryptologic services. In addition to this, it is important that any plan proposed should provide the maximum possible protection against the effects of partial penetration of either type.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

10. Properly-constructed one-time pad systems would provide the necessary security but it does not appear feasible to recommend such a solution even for the French Diplomatic communications alone. The cumbersome operational characteristics of such systems and the labor required to prepare and distribute the pads in the required quantity would probably make a proposal of this kind unacceptable to the French. Likewise, the provision of modern secure machine systems in the quantity required for use in the Foreign Ministry and in all important diplomatic posts would probably be beyond the financial capacity of the French Government at this time. Nor can the United States undertake the supplying of materials or equipment on the required scale.

11. The AFSA plan proposed in Enclosure "A" is a reasonable and economical program for providing adequate cryptographic security for the various levels of French Diplomatic and Military communications. The plan will, if properly executed, effectively prevent the production of a significant amount of communication intelligence therefrom. The plan is divided

into two parts: A- For Diplomatic communications, and B- For the communications of the Armed Services. Part B has been coordinated with the plan now under study by authorities concerned with NATO communications. The latter, however, have thus far concerned themselves only with communications of two levels directly connected with NATO matters; they have not concerned themselves with purely national communications having at present no bearing on NATO matters. The purely national communications may be regarded as constituting a third level of communications, which in the case of France would also require increased security protection in war time, and which are therefore also provided for in the present AFSA plan.

12. The bases for, and the steps to be taken in approaching the French Government, with a view toward improving the security of French communications, will constitute one of the important matters to be discussed at the forthcoming U.S.-U.K. conference in Washington.

Mr. Friedman
20 April

DRAFT

STAFF STUDY ON THE IMPROVEMENT OF FRENCH COMMUNICATIONS

THE PROBLEM

1. In preparation for a US-UK conference on the subject, to examine present French cryptographic systems and procedures, and to formulate a U.S. plan for improvement of the security thereof.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure "B."

CONCLUSIONS

3. It is concluded that:

[redacted]

b. The present French cryptographic organizations do not possess the necessary cryptanalytic appreciation to insure provision of systems affording adequate cryptographic security, or, if they do possess the requisite knowledge, the information is not being applied or properly employed.

c. This situation can be corrected only by a complete overhaul of the French cryptographic systems and practices. The present insecure French cryptographic systems and practices should be replaced by secure systems and practices, and a specific plan for such replacement should be established.

d. Positive measures to effect such a plan should be introduced even to the extent of providing, at least in part, the cryptographic devices and associated techniques essential to security.

e. This will materially reduce the amount of intelligence now available to Russia from COMINT sources probably exploitable by them; it

[redacted]

f. Negotiations with the French should be conducted in such a manner that there is [redacted]

g. As a preliminary to entering upon any negotiations with the French there should be reasonable assurance that the effects of improving their communication security will not be nullified or diminished by physical and personnel insecurity in the French Government. It is obvious that without such assurance [redacted] without any compensating gains in security.

h. The bases for a successful approach to the French Government cannot yet be indicated and should be established in the discussions at the U.S.-U.K. Conference soon to convene in Washington.

ENCLOSURE "A"

PLAN FOR IMPROVING THE CRYPTOGRAPHIC SECURITY OF FRENCH COMMUNICATIONS

A. DIPLOMATIC:

1. The proposal presented herein for ensuring the security of French Diplomatic communications considers that the various French diplomatic posts should be subdivided into three categories:

a. Category I: A small group of locations which handle the most critical information, such as Paris, London, and Washington.

b. Category II: All capitals not included in a. plus a selected group of important cities whose communications frequently include information of considerable intelligence value.

c. Category III: All other diplomatic posts.

2. The systems recommended, respectively, for the three categories listed above are:

a. For Category I: The Combined Cipher Machine with Simplex settings. The word Simplex is used to mean a procedure whereby each message has its own rotor arrangement and alignment provided by means of a special key list. The lists are prepared for point-to-point use so that each station can read only those messages specifically addressed to it. For the exceptional cases of multiple-address messages, a multiple holder key list is provided. A one-time pad system should be provided as an emergency stand-by in this category.

b. For Category II: The M-209 with special settings used to encipher messages set up in a literal code. The code book used should be a new book specially designed for this sole purpose. Each holder in this category should be provided with three distinct systems; one for use solely with Paris, one for use laterally on a limited regional basis, and one for use laterally on a world wide basis.

c. For Category III: Present French systems would continue to be used.

3. The stations in each category will be included as holders in the categories below them.

4. The localization introduced by Simplex procedures in Category I and by special or area settings in Category II has a double advantage. First, it increases the cryptosecurity generally; and secondly, if there should be an instance of penetration by the Russians which grants access to cryptographic information, the dangers resulting from such penetration are confined to the single cryptonet involved. This results in minimizing the consequent loss of information.

5. The merit of these proposals is the provision of a fairly high degree of security for French Diplomatic and highest-level NATO communications, together with a minimum disclosure to the French of systems and ideas with which they are not already familiar. For the transmission of international Diplomatic or highest-level Military traffic dealing with Western Union and NATO affairs, they have been provided with TYPEX machines and they are presently using a Simplex procedure with these machines in the highest echelons of NATO; the Combined Cipher Machine is also being offered to them, as well as to other NATO signatories, for NATO communications; French Army, Navy, and Air Force personnel are familiar with and have some copies of the M-209, so that they have experience in the preparation of M-209 settings and can instruct French diplomatic officials in the use of the M-209. Adequate training in the new systems will therefore be greatly simplified as a result of the already-existing familiarity with them.

6. The establishment of appropriate communications security procedures will be facilitated by the issue of JANAP 122(B) (the U.S. Joint Manual on Communications Security), which is presently under consideration for use in connection with NATO cryptographic systems.

B. ARMED SERVICES:

7. Authorities concerned with NATO communications have already established two categories of such communications:

a. Category I (High-level): This category embraces the top-level military representatives of each nation of NATO. For this level, the British TYPEX machine, with Simplex settings is being used. Consideration is being given to adapting that machine to a NATO CCM system.

b. Category II (Intermediate-level): This category embraces military headquarters down to and including Division headquarters or equivalent. For ~~the~~ this level the U.S. and the U.K. have proposed the CCM, and the proposal is now under consideration by the other NATO governments.

8. There remains for consideration purely French national military (Army, Navy, Air Force) communications of ~~a~~ the level of 7b and below, ~~that of 7b above~~. For this level, which would constitute Category III, the use of M-209, to encipher plain language (not code groups as in the case of Category II of the plan for the Diplomatic communications provided for in paragraph 2b above) would probably be acceptable to the U.S.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

[redacted]

2. In regard to the current French Diplomatic communications, observed French practices in cryptographic system design and distribution provide direct evidence that the present cryptographic organization in the French Diplomatic Service does not possess the necessary cryptanalytic appreciation to insure provision of systems affording adequate cryptographic security, or, if it does possess the requisite knowledge, the information is not being applied or properly employed, either in the Foreign Ministry or in Diplomatic posts. Except as regards certain systems, which may be one-time pad, none of the French Diplomatic cryptographic systems possesses sufficient inherent security to permit its improvement to a point where it might be considered acceptable. It would therefore be necessary to discard the current systems

and replace them with other systems based on sounder cryptographic principles. It would also be necessary to provide technically sound associated procedures and training in the proper use of the systems and procedures.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

4. Although a tradition of sound communication security doctrine did exist in France, the current cryptographic practices observed in French Diplomatic traffic indicate that the French have fallen far behind the U.S. and the U.K. in matters pertaining to communication security. The situation is less serious in the Army, but there too there is much room for improvement. Therefore, technical assistance from outside the French cryptographic services is deemed essential for the success of any communication security program.

5. From an over-all consideration it may be stated that if the security of French Diplomatic and Military communications is to be improved it would be necessary to:

a. Replace the current French cryptographic systems with secure systems for use in all important diplomatic posts and in the headquarters of all high-echelon military units.

b. Establish technically sound communications security procedures.

c. Insure adequate training in the use of the new systems and procedures.

d. Insure careful technical supervision over French communications to maintain communication security.

6. In view of the foregoing, it is apparent that a complete overhaul of the French Diplomatic and Military cryptographic systems and practices would be necessary. This would involve not only informing the French that their present systems are insecure but also establishing a basis on which the French would be provided with appropriate technical assistance to enable them to reorganize their cryptographic systems and practices to insure secure communications.

7. It is obvious that in assisting the French in improving the security of their cryptographic communications [redacted] However, (a) the necessity for removing those handicaps to proper diplomatic discussions and negotiations between the U.S. and the French Governments which arise from present insecurity of French Diplomatic communications, and (b) the importance of denying to Russia this source of COMINT, make it in the interest of the U.S. and the U.K. to accept a complete loss of COMINT from French sources and also to provide, at least in part, the cryptographic devices and associated techniques essential to security.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

9. The possibility of Russian penetration of some or all of the French services, both diplomatic and military, cannot be ignored. Penetration may be either complete or partial, and may extend into either the sources of information or into the cryptographic services. Complete penetration of either type would make totally ineffective any plan for improving cryptographic security. [redacted] without denying information to the Russians. Therefore, before any steps are taken, there should be reasonable assurance of adequate physical and personnel security in the French Foreign Office, the French Armed Services, and the offices which control the cryptologic services. In addition to this, it is important that any plan proposed should provide the maximum possible protection against the effects of partial penetration of either type.

10. Properly-constructed one-time pad systems would provide the necessary security but it does not appear feasible to recommend such a solution even for the French Diplomatic communications alone. The cumbersome operational characteristics of such systems and the labor required to prepare and distribute the pads in the required quantity would probably make a proposal of this kind unacceptable to the French. Likewise, the provision of modern secure machine systems in the quantity required for use in the Foreign Ministry and in all important diplomatic posts would probably be beyond the financial capacity of the French Government at this time. Nor can the United States undertake the supplying of materials or equipment on the required scale.

11. The AFSA plan proposed in Enclosure "A" is a reasonable and economical program for providing adequate cryptographic security for the various levels of French Diplomatic and Military communications. The plan will, if properly executed, effectively prevent the production of a significant amount of communication intelligence therefrom. The plan is divided

into two parts: A- For Diplomatic communications, and B- For the communications of the Armed Services. Part B has been coordinated with the plan now under study by authorities concerned with NATO communications. The latter, however, have thus far concerned themselves only with communications of two levels directly connected with NATO matters; they have not concerned themselves with purely national communications having at present no bearing on NATO matters. The purely national communications may be regarded as constituting a third level of communications, which in the case of France would also require increased security protection in war time, and which are therefore also provided for in the present AFSA plan.

12. The bases for, and the steps to be taken in approaching the French Government, with a view toward improving the security of French communications, will constitute one of the important matters to be discussed at the forthcoming U.S.-U.K. conference in Washington.